

Joiners, Movers, Leavers — and Watching the Accounts In Between

Sat, Aug 8, 2:00 PM EDT · <https://scottslab.io/posts/provisioning-deprovisioning-account-monitoring>



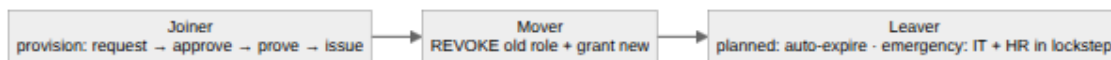
TL;DR

The account lifecycle has three moments that matter: provisioning a joiner, moving someone (where you must revoke the old role, not just add the new), and deprovisioning a leaver. Planned exits should auto-expire on the last day; emergency terminations need IT and HR timed to the minute. Too early tips the person off, too late leaves them access. Continuous monitoring watches for the tells: impossible travel, odd hours, and bulk downloads.

Every account has a beginning, a middle, and an end, and each transition is a place security quietly gets lost.

Provisioning a joiner is the easy one, and it's the registration-and-separation-of-duties process from earlier in this series: request, approve, prove, issue. The interesting failures come later.

The mover is the transition everyone botches. When someone changes roles, adding their new permissions is what unblocks them, so that always happens; revoking the permissions from their old role unblocks nobody, so it quietly doesn't. Do that a few times per employee and you've hand-built privilege creep. An internal transfer has to be handled as a revoke-and-grant, never just a grant.



The leaver is where timing becomes everything. A planned departure is clean: set the account to expire automatically on the last day and nobody has to remember. An emergency termination is the hard case, because IT and HR have to move in lockstep. Cut access too early and the person notices they're locked out before anyone has spoken to them. That's advance warning to someone who may want to retaliate. Cut it too late and a just-fired employee still holds the keys. The entire exercise is collapsing that window toward zero, which only happens when HR and IT are working off the same clock.

Once accounts are live, monitoring is how you catch the ones that have been taken over or turned malicious. The useful signals are behavioral, not failed logins. Impossible travel: one account authenticating from two places too far apart to be real. Logins from networks or at hours that don't fit the person. Bulk file access or downloads that look like someone emptying the drawers on the way out. Location sharpens all of it. Geotagging and geofencing turn "unusual place" from a hunch into a rule.

